REMARKS

Claims 53 and 70 are amended. No new claims are added. Claims 1-94 are pending for consideration. In view of the following amendments and remarks, Applicant respectfully requests that this application be allowed and forwarded on to issuance.

Objections to the Drawings

Figure 1 of the Drawings is objected to because, in the opinion of the Office, only that which is old is illustrated (page 2 of Office action). Accordingly, a replacement sheet compliant with 37 CFR 1.121, including an amended Fig. 1, is being filed contemporaneously with this Response. Specifically, the amended Fig. 1 includes the text "PRIOR ART" and is labeled "REPLACEMENT SHEET" within the header portion thereof. The Applicant believes that such amendment/replacement sheet fully satisfies the objection raised by the Office and therefore respectfully requests that the objection to the Drawings be withdrawn. No new matter has been submitted by way of the replacement sheet for Figure 1.

§ 112 Rejections

Claims 53-86 stand rejected under 35 U.S.C. § 112, Second Paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicant regards as the Invention. Specifically, independent claims 53 and 70 are respectively rejected under § 112 because each recites, in salient part: "a decryptor that is uniquely **able to** decrypt...", wherein the claim language "able to" is alleged by the Office as a non-positive limitation (Page 2 of Office action). Claims 54-69 and 71-86 are rejected under § 112 by virtue of their

respective dependencies from claims 53 and 70. Applicant disagrees with the Office's rejections and maintains that the claims are fine as they appear. Nonetheless, in the spirit of cooperation and in the interest of advancing the pending application to allowance, independent claims 53 and 70 have been amended as indicated above.

Specifically, claims 53 and 70 have been respectively amended to recite, in salient part: "a decryptor that is uniquely **configured so as** to decrypt...", thus deleting the language "able to" from the claim. The Applicant believes the respective amendments to independent claims 53 and 70 fully address the rejections under § 112 asserted by the Office, and respectfully requests that these rejections be withdrawn. As claims 54-69 and 71-86 respectively depend from claims 53 and 70, as respectively amended, the Applicant request that the § 112 rejection also be withdrawn. No new matter has been introduced through the amendments to the claims.

§ 102 and § 103 Rejections

Claims 23, 26-27, 30-31, 34-35, 38-39, 41 and 44 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2005/0102264 ("Nason").

Claims 1-2, 5-8, 11-13, 16-20, 40, 42, 45, 48-50 and 52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason, in view of U.S. Patent Application Publication No. 2002/0136408 ("Garcia").

Claims 3-4, 14-15 and 46-47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Garcia, in further view of U.S. Patent No. 5,727,062 ("Ritter").

Claims 9-10 and 20-21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Garcia, in further view of U.S. Patent No. 5,572,235 ("Mical").

Claims 24-25, 32-33 and 43 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Ritter.

Claims 28-29 and 36-37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Mical.

Claim 51 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Garcia, in further view of U.S. Patent No. 6,934,389 ("Strasser").

Claims 53-56, 59, 63-66, 69-73, 76, 80-83 and 86 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Strasser.

Claims 87, 89-92 and 93-94 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Garcia, in further view of Strasser.

Claims 57-58, 74-75 and 88 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Strasser, in further view of Ritter.

Claims 60-62 and 77-79 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Strasser, in further view of Garcia.

Claims 60-62 and 77-79 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Strasser, in further view of Garcia.

Claims 67-68 and 84-85 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Nason in view of Strasser, in further view of Mical.

The Claims

Claim 1 recites a method comprising:

- decrypting encrypted data that resides on one or more memory surfaces associated with a video card, said act of decrypting being performed under the influence of ***a cryptographic processor that resides on the video card***, said act of decrypting taking place only when an operation is to be performed on the data by ***a graphics processor unit (GPU) that resides on the video card***;
- ***performing an operation on the decrypted data using the GPU to provide resultant data***;
- ***re-encrypting, under the influence of the cryptographic processor, the resultant data***; and
- writing the encrypted resultant data to a memory surface associated with the video card.
- ***at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.***

[***Emphasis added.***]

In making out the rejection of this claim, the Office argues that its subject matter rendered obvious by the combination of Nason with Garcia. Applicant respectfully disagrees and traverses the Office's rejection. For the reasons set forth below, the rejection over the combination of Nason and Garcia does not establish a prima facie case of obviousness.

First, the Office relies upon Garcia for a disclosure (i.e., teaching) that in fact is not present. Thus, the combination of Nason and Garcia fails to teach or suggest at least one feature as positively recited in the claimed subject matter.

Second, the Office asserts a modification to the teachings of Nason in view of the alleged teachings of Garcia that would change the principle of operation of the Nason reference. Such a modification is impermissible under MPEP § 2143.01(VI). Each of these arguments will be addressed below under separate subheadings.

A. Failure to Disclose Claimed Subject Matter

The Office argues that Nason discloses essentially all of the subject matter of claim 1, *except* for the act of "decrypting being performed under the influence of a cryptographic processor that resides on the video card" (page 6 of Office action). For this feature, the Office relies on Garcia. Respectfully, the Office is in error with respect this point as described below.

Specifically, Nason fails to teach or suggest a cryptographic processor that resides on the video card, as positively recited by this claim. Such has already been admitted by the Office. However, Nason also fails to teach or suggest performing an operation on the decrypted data using the GPU to provide resultant data, and re-encrypting, under the influence of the cryptographic processor, the resultant data, as positively recited by claim 1. Furthermore, Nason fails to teach or suggest at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis, as positively recited by claim 1.

Rather, Nason specifically teaches methods and systems for preventing the unauthorized access, interception and/or modification of computer code on a client device and, among other things, such data as pertaining to graphical information resident in VRAM of a video card (Abstract, *et seq.* of Nason). However, it is important to note that under every procedure or method taught by Nason - pertinent in any way to information resident on a video card - a Security Enhanced Display Driver (SEDD) plays an essential role in the "scheduling" (i.e., control, derivation, provision and/or exchange) of secured data. For example, paragraph 0011 of Nason recites:

> "In one embodiment, a security enhanced display driver (SEDD) is provided to schedule content of portions of a frame buffer stored in a video

display memory. In one such embodiment, a request to display data to a secure region on a video display made to the SEDD. In response, the SEDD *allocates* a corresponding secure portion of the frame buffer and *schedules* the data content of this secure portion such that valid data is only present in the secure portion at the time it is needed for projection to the display device and when other tasks are locked out of accessing (reading or writing) to the secure portion. The SEDD *determines*, depending upon, the obfuscation techniques used, when data stored in the secure portion needs to be de-obfuscated and when it needs to be re-obfuscated."

[Emphasis added.]

Nason groups the SEDD together within all other drivers, software and the operating system used by the client computer to be kept secure (Fig. 1 of Nason). Nason further makes it clear that the operating system, display driver (i.e., SEDD), and other software reside and are utilized by a processor **away from** both the video card and any VRAM resident thereon (Figs. 2 and 4 of Nason). Thus, Nason exclusively teaches that: 1) an SEDD is not part of any video card; yet is 2) essential to any and all security measures taken with respect to a video card.

In no way does Nason teach or suggest a **cryptographic processor that resides on the video card**, as recited by claim 1. Also, Nason fails to teach or suggest **re-encrypting, under the influence of the cryptographic processor, the resultant data** (as provide by operation of a GPU), as recited by claim 1. To this extent, Nason teaches directly away from any such notion.

Further still, Nason is completely devoid of any teachings or suggestion related to an act of **decrypting or re-encrypting on a per cache page basis**. To this particular point, Nason makes no mention whatsoever of a "cache page", "cache", or any of their respective equivalents. More to the point, Nason expresses no concern at all for any cache (of a GPU or otherwise) or any operations performed in such a context. If anything, Nason teaches measures that

are performed with respect to secure ***portions*** of information, eventually resident in VRAM, under the control of an SEDD (Para. 0056 of Nason). The Office is respectfully referred to page 26, lines 1-23 of the Specification as originally filed for clarifying information in this regard.

Garcia fails to cure the deficiencies of Nason. Specifically, Garcia fails to teach or suggest a cryptographic processor that resides on the video card, as positively recited by this claim. Also, Garcia fails to teach or suggest performing an operation on the decrypted data using the GPU to provide resultant data, and re-encrypting, under the influence of the cryptographic processor, the resultant data, as positively recited by claim 1.

Rather, Garcia teaches *particular* encryption algorithms of variable block lengths, as applied to graphical data (Abstract, Paragraphs 0036-0041, *et seq.* of Garcia). Garcia then briefly mentions that these specific algorithms - as are the true focus of Garcia - can be implemented by way of, for example, "graphics cards with encryption facilities", and "Graphic Processing Unit (GPU) devices with encryption facilities" (Paragraphs 0074-0075 of Garcia). However, Garcia does not provide any insight as to particular embodiments or respective details of the forgoing. The Office is respectfully referred to MPEP 2121.01, which states, in pertinent part:

> "The disclosure in an assertedly anticipating reference must provide an ***enabling disclosure*** of the desired subject matter; ***mere naming or description of the subject matter is insufficient, if it cannot be produced without undue experimentation***. *Elan Pharm., Inc. v. Mayo Found. For Med. Educ. & Research*, 346 F.3d 1051, 1054, 68 USPQ2d 1373, 1376 (Fed. Cir. 2003)." [Emphasis added.]

In view of the foregoing provisions of the MPEP, the Applicant asserts that Garcia is lacking sufficient enablement to serve as an enabling (i.e., sufficient) reference as Garcia has been applied by the Office.

Furthermore, Garcia asserts that the specific algorithms taught thereby – and does not suggest that any others - are suitable for implementation by such casually mentioned means. Such nebulous hinting by Garcia is in stark contrast to the particular teachings of the pending Application, especially at Figs. 5 and 6 of the Drawings, and at page 17, line 15 to page 20, line 15 of the Specification, as respectively originally filed.

In any case, Garcia specifically fails to teach or suggest a video card, including a graphics processing unit GPU ***and*** a cryptographic processor resident thereon, as specifically recited by the subject matter of claim 1. Furthermore, Garcia fails to teach or suggest **re-encrypting, under the influence of the cryptographic processor, the resultant data** (as provide by operation of a GPU), as recited by claim 1. Garcia is exclusively concerned with particular algorithms for providing secured data content in a specific way. Moreover, Garcia is lacking any teaching or suggestion with regard to a **cache page**, or any operations performed on such a basis.

There is no way to select elements from Nason, and then to somehow combine those elements with other elements taken from Garcia, in order to arrive at the subject matter recited by claim 1, as no possible combination of Nason and Garcia teaches or suggests all of the required features. At the very least, any such combination of Nason and Garcia is completely lacking: 1) a video card including a graphics processor unit and a cryptographic processor resident thereon; 2) re-encrypting, under the influence of the cryptographic processor, resultant data from

an operation of the GPU; and 3) any operation performed on a per cache page basis.

Accordingly, the Office's *prima facie* case of obviousness fails for at least the reason that the combination of Nason and Garcia fails to teach or suggest all of the features recited in the claimed subject matter.

B. Impermissible Modification to Principle of Operation

Assuming *arguendo* that Nason, when combined with Garcia, *does* teach all of the required features (which it does not), the Office attempts an impermissible modification to the teachings of Nason in order to arrive at the subject matter of claim 1.

To begin, the Applicant asserts that Nason contemplates *only* those security measures that are implemented by way of conventional, widely-known video card technology under the control of a security-enhanced driver (SEDD), and that such is fundamental to the principle of operation of the Nason teachings. That is, the SEDD of Nason operates by way of a corresponding microprocessor of the client computer from a location off the video card. Thus, the Applicant further contends, any encrypted or decrypted data under Nason is derived by way of microprocessor operations separate and apart from any video card, wherein such data is subsequently communicated to such a video card.

The Office then asserts (wrongly) that, in view of the teachings of Garcia, it would be obvious to:

> "modify the method disclosed in Nason et al. to incorporate the cryptographic processor within the GPU which is located on the graphics card. This modification would have been obvious because a person having

ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Garcia suggests that incorporating cryptographic capabilities within the GPU make performing cryptographic functions easier and is not costly." (page 6 of Office action)

This is assertion is flawed, and any modifications to Nason there under are impermissible, for at least the following reasons:

1) Nason, as explained above, *exclusively* teaches methods and systems founded on a conventional video card under the control of a proprietary driver – namely, an SEDD. Thus, the any modification to Nason resulting in the shifting of the performance of such security measures (encryption, decryption, etc.), or any other related operations, from off-card SEDD control to a cryptographic processor on a video card constitutes a ***fundamental and material change in the operating principle*** of Nason, that is neither taught nor suggested by the Nason reference. In view of MPEP § 2143.01(VI), such a change is not allowed and an assertion for *prima facie* obviousness cannot be supported thereby.

2) The motivation for the proposed modification expressed by the Office has no bearing on, and is neither taught nor suggested by, the concerns discussed within Nason. Specifically, Nason expresses no concern with respect to the cost of implementing the sort of security features (i.e., the SEDD) taught thereby. Likewise, Nason expresses no concern for the ease of implementation of the SEDD or any related driver. Thus, there is no motivation to be found anywhere within Nason to suggest that less costly or easier-to-implement solutions should be pursued. From all indications - or rather, the complete lack thereof - Nason is fully satisfied as to the economy and straightforwardness of the solutions presented therein.

3) As explained above, neither Nason nor Garcia teaches or suggests the particular sort of cryptographic processor needed in order to perform the subject matter as recited by claim 1. Furthermore, neither Nason nor Garcia teaches or suggests all of the particular operations as recited by the subject matter of claim 1. Thus, *even if* there were legitimate support within Nason to permit the sort of modifications thereto asserted by the Office (which there is not), neither Nason nor Garcia provides, teaches or suggests the overall specific, synergistic form and functionality that would be required.

Accordingly, the Office's *prima facie* case of obviousness fails for at least the reason that the proposed modifications to the teachings of Nason are impermissible and lacking adequate support within Nason and Garcia. For at least the foregoing reasons, the Applicant asserts that claim 1 is allowable.

Claims 2-11 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 2-11 have been considered, none are seen as expressing anything of merit.

Claim 12 recites a method comprising:

- ***decrypting encrypted data*** that resides on one or more memory surfaces associated with a video card, ***said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card***, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;
- ***performing an operation on the decrypted data using the GPU to provide resultant data***;
- ***re-encrypting, under the influence of the cryptographic processor, the resultant data***; and
- ***writing the encrypted resultant data to a memory surface associated with the video card***;

- ***said acts of decrypting and re-encrypting taking place on a per cache page basis.***

[***Emphasis added.***]

In making out the rejection of this claim, the Office argues that its subject matter is rendered obvious by the combination of Nason with Garcia. Applicant respectfully disagrees and traverses the Office's rejection. For the reasons set forth below, the rejection over the combination of Nason and Garcia does not establish a *prima facie* case of obviousness.

First, the Office relies upon Garcia for a disclosure (i.e., teaching) that in fact is not present. Thus, the combination of Nason and Garcia fails to teach or suggest at least one feature as positively recited in the claimed subject matter.

Second, the Office asserts a modification to the teachings of Nason in view of the alleged teachings of Garcia that would change the principle of operation of the Nason reference in manner that is not permitted.

In the first place, Nason neither teaches nor suggests decrypting encrypted data, said act of decrypting being performed under the influence of a cryptographic processor that resides on the video card, as positively recited by the subject matter of claim 12. The Office has admitted to this deficiency of Nason (page 8 of Office action). However, Nason also fails to teach or suggest performing an operation on the decrypted data using the GPU to provide **resultant data**, as positively recited by the subject matter of this claim. Nason further fails to teach or suggest re-encrypting, under the influence of the cryptographic processor, the resultant data, and writing the encrypted resultant data to a memory surface associated with the video card, as positively recited by the subject matter of claim 12. Furthermore, Nason fails to teach or suggest said acts of decrypting

and re-encrypting taking place on a per cache page basis, as positively recited by the subject matter of this claim.

Rather, Nason teaches that the graphics processing unit (GPU) thereof is used for "projecting" video data to the display unit (screen). More particularly, the GPU transfers data (bits, etc.) from a frame buffer 204 within VRAM 203 to a display 220 so that a corresponding image is provided to a user (Fig. 2; Para. 0047 of Nason). Under Nason, the GPU can also "OR" or "XOR" data from different storage locations in memory so that an overall combined image frame is sent to the display (*Id.*). Thus, as taught by Nason, the GPU serves to gather graphical data from one or more storage locations (virtual buffers in VRAM), assemble that data into a meaningful whole (if necessary), and provide that data directly *and exclusively* to the corresponding user display.

However, Nason does not provide, teach or suggest that any GPU is used to perform an operation on decrypted data such that resultant data is derived, wherein the resultant data is then re-encrypted. Nason is concerned with storing graphical data in either its original form, or in an encrypted or otherwise "obfuscated" derivation of its original form, until it is needed for projection to the display by the GPU. Nason does not teach or suggest the re-encryption or other "re-obfuscation" of resultant data that has been processed (operated upon) by the GPU such that the resultant data is now changed with respect to its original, pre-operation form or content. Also, and as argued above in regard to claim 1, Nason is totally lacking any teaching or suggestion with respect to a cache page, or *any* operations performed on a per cache page basis.

Garcia fails to cure the deficiencies of Nason. Specifically, Garcia fails to teach or suggest decrypting encrypted data, said act of decrypting being performed

under the influence of a cryptographic processor that resides on the video card, as positively recited by the subject matter of claim 12. Again, Garcia teaches on those specific algorithms of interest to Garcia, and then briefly suggests (without enabling detail) means for performing such particular algorithms – nothing more. Furthermore, Garcia fails to teach or suggest any of: performing an operation on the decrypted data using the GPU to provide resultant data; re-encrypting, under the influence of the cryptographic processor, the resultant data; writing the encrypted resultant data to a memory surface associated with the video card; or said acts of decrypting and re-encrypting taking place on a per cache page basis, as respectively and positively recited by the subject matter of claim 12. Therefore, no possible combination of Nason with Garcia teaches or suggests all of the features of the subject matter of claim 12.

In the second place, *even if* some combination of Nason with Garcia taught or suggested all of the required elements (and in fact, no such combination exists), any such modification as proposed by the Office (page 8 of Office action) would not be permitted under MPEP § 2143.01(VI) because an impermissible change in the operating principle of Nason would be required. The Office is respectfully directed to the reasons argued above in regard to claim 1, as such are analogous and supportive in regard to claim 12.

For at least the foregoing reasons, the § 103 rejection of claim 12 is unsupportable and must be withdrawn. The Applicant asserts that clam 12 is allowable.

Claims 13-22 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 13-22 have been considered, none are seen as expressing anything of merit.

Claim 23 recites a method comprising:

- decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;
- ***performing an operation on the decrypted data using the GPU to provide resultant data;***
- ***re-encrypting the resultant data***; and
- ***writing the encrypted resultant data to a video card memory surface associated with the video card,***
- ***at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.***

[***Emphasis added.***]

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Nason. Applicant respectfully disagrees and traverses the Office's rejection. For the reasons set forth below, the rejection over Nason does not support a rejection based on anticipation.

Specifically, Nason fails to provide performing an operation on the decrypted data using the GPU to provide resultant data as positively recited by the subject matter of this claim. Also, Nason fail to provide for either of re-encrypting the resultant data, or writing the encrypted resultant data to a video card memory surface associated with the video card, as positively recited by the subject matter of claim 23. Furthermore, Nason fails to provide at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis, as positively recited by the subject matter of claim 23.

Specifically, and substantially as argued above in regard to claim 12, Nason expresses no concern for performing an on operation on decrypted data – using a

GPU, or any other means - such that resultant data is derived, and then re-encrypting the resultant data. Rather, Nason is concerned with encrypting (obfuscating) data directly from its original form for purposes of maintaining security against unauthorized parties, and then decrypting such data only when necessary for projection to a user display.

In any case, Nason does not express any means for or procedural sequences including: 1) decrypting encrypted data; 2) performing an operation on the decrypted data, using a GPU, to derive resultant data; and 3) re-encrypting the resultant data and writing it to a memory surface. Further still, Nason expresses no concern for any sort decrypting and/or re-encrypting performed on a per cache page basis.

For at least the foregoing reasons, Nason fails to provide at least one feature as positively recited by this claim. Accordingly, the anticipation rejection of claim 23 is unsupportable and must be withdrawn. In turn, claim 23 is allowable.

Claims 24-30 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 24-30 have been considered, none are seen as expressing anything of merit.

Claim 31 recites a method comprising:

- decrypting encrypted data that resides on one or more memory surfaces of a video card memory, said act of decrypting taking place only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;
- ***performing an operation on the decrypted data using the GPU to provide resultant data***;
- ***re-encrypting the resultant data***; and
- ***writing the encrypted resultant data to a video card memory surface associated with the video card,***
- ***said acts of decrypting and re-encrypting taking place on a per cache page basis.***

[*Emphasis added.*]

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Nason. Applicant respectfully disagrees and traverses the Office's rejection. For the reasons set forth below, the rejection over Nason does not support a rejection based on anticipation.

Specifically, Nason fail to provide performing an operation on the decrypted data using the GPU to provide resultant data, as positively recited by the subject matter of this claim. Also, Nason fails to provide re-encrypting the resultant data, and writing the encrypted resultant data to a video card memory surface associated with the video card, as positively recited by the subject matter of this claim. Further, Nason fails to provide said acts of decrypting and re-encrypting taking place on a per cache page basis, as positively recited by the subject matter of claim 31. For reasons analogous to those argued above in regard to claim 12, Nason fails to provide at least one feature as positively recited by this claim. Accordingly, the anticipation rejection of claim 31 is unsupportable and must be withdrawn. In turn, claim 31 is allowable.

Claims 32-38 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 32-38 have been considered, none are seen as expressing anything of merit.

Claim 39 recites a system comprising:

- ***means for decrypting, on a per cache page basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card;***

- ***means for performing an operation on the decrypted data to provide resultant data;***
- ***means for re-encrypting, on a per cache page basis, the resultant data***; and
- ***means for writing the encrypted resultant data to a video card memory surface associated with the video card.***

[***Emphasis added.***]

In making out the rejection of this claim, the Office argues that its subject matter is anticipated by Nason. Applicant respectfully disagrees and traverses the Office's rejection. For the reasons set forth below, the rejection over Nason does not support a rejection based on anticipation.

Specifically, Nason fails to provide means for decrypting, on a per cache page basis, encrypted data that resides on one or more memory surfaces of a video card memory only when an operation is to be performed on the data by a graphics processor unit (GPU) that resides on the video card, as positively recited by the subject matter of this claim. Also, Nason fails to provide means for performing an operation on the decrypted data to provide resultant data, as positively recited by the subject matter of claim 39. Nason fails to provide means for re-encrypting, on a per cache page basis, the resultant data, as positively recited by the subject matter of this claim. Furthermore, Nason fails to provide means for writing the encrypted resultant data to a video card memory surface associated with the video card, as positively recited by the subject matter of this claim.

As argued above, Nason makes no provision for any means for, nor any procedure regarding: 1) anything performed on a per cache page basis; or 2) any operations on decrypted data to provide resultant data; 3) re-encrypting such resultant data; or 4) writing encrypted resultant data to a video card memory

surface. For at least these reasons, Nason fails to provide at least one feature as positively recited by this claim. Accordingly, the anticipation rejection of claim 39 is unsupportable and must be withdrawn. In turn, claim 39 is allowable.

Claims 40-44 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 40-44 have been considered, none are seen as expressing anything of merit.

Claim 45 recites a system comprising:

- a video card;
- a graphics processor unit (GPU) on the video card and configured to process video data that is to be rendered on a display device;
- ***memory on the video card comprising*** one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and ***one or more output memory surfaces configured to hold encrypted resultant data*** that is to be rendered on the display device;
- ***a cryptographic processor on the video card and configured to control encryption and decryption on the video card***, the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted, on a per cache page basis, in connection with an operation that is to be performed on the data by the GPU; and
- ***the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted, on a per cache page basis, to an output memory surface.***

[*Emphasis added.*]

In making out the rejection of this claim, the Office argues that its subject matter is rendered obvious by the combination of Nason with Garcia. Applicant respectfully disagrees and traverses the Office's rejection. For the reasons set forth below, the rejection over the combination of Nason and Garcia does not establish a *prima facie* case of obviousness.

First, the Office relies upon Garcia for a disclosure (i.e., teaching) that in fact is not present. Thus, the combination of Nason and Garcia fails to teach or suggest at least one feature as positively recited in the claimed subject matter.

Second, the Office asserts a modification to the teachings of Nason in view of the alleged teachings of Garcia that would change the principle of operation of the Nason reference in manner that is not permitted.

As to the first matter, Nason fails to teach or suggest a cryptographic processor on the video card and configured to control encryption and decryption on the video card, as positively recited by the subject matter of this claim. Such deficiency on the part of Nason has been admitted by the Office (page 11 of Office action). However, Nason fails to teach or suggest memory on the video card comprising one or more output memory surfaces configured to hold **encrypted resultant data**, as positively recited by the subject matter claim 45. Also, Nason fails to teach or suggest the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted, on a **per cache page basis**, to an output memory surface, as positively recited by the subject matter of this claim.

Nason expresses no concern for resultant data, as that term applies in the context of claim 45, and Nason does not suggest an encrypted form of such resultant data. Also, Nason is lacking any teachings regarding any operation or means going to a per cache page basis. Frankly, Nason is directed to substantially different means and methods of operation, than the subject matter as recited by claim 45.

Garcia fails to cure the deficiencies of Nason. Specifically, Garcia fails to teach or suggest a cryptographic processor on the video card and configured to

control encryption and decryption on the video card, as positively recited by the subject matter of this claim. As argued above, Garcia makes only broad, off-hand suggestions as to the means to be employed to perform the specific algorithms of Garcia. Garcia does not teach or suggest the particular cryptographic processor, nor its configuration, as recited by the subject matter of claim 45. Also, Garcia is lacking any teachings or suggestions directed to memory on the video card comprising one or more output memory surfaces configured to hold encrypted resultant data, or the cryptographic processor further being configured to enable data that has been operated upon by the GPU to be encrypted, on a per cache page basis, to an output memory surface, as positively recited by the subject matter of this claim. Therefore, no possible combination of Nason and Garcia provides all of the features as recited by the subject matter of claim 45.

As to the second matter, MPEP § 2143.01(VI) does not permit the modification to Nason as suggested by the Office (page 11 of Office action) in order to arrive at the subject matter of claim 45 – regardless of the particular teachings of Garcia (which are deficient as argued above) – as such modification would change a *principle of operation* of Nason.

For at least the forgoing reasons, the Office has failed to support a *prima facie* obviousness rejection against claim 45. Therefore, the Applicant asserts that claim 45 is allowable.

Claims 46-52 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 46-52 have been considered, none are seen as expressing anything of merit.

Claim 53 has been amended, and as amended recites a method comprising [added text is emphasized by underlining]:

- providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;
- ***associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface***;
- decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;
- ***performing an operation on the decrypted data using the GPU to provide resultant data***;
- ***re-encrypting the resultant data***; and
- ***writing the encrypted resultant data to an output memory surface associated with the video card,***
- ***at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis.***

[***Emphasis added.***]

In making out the rejection of this claim, the Office argues that its subject matter rendered obvious by the combination of Nason with Strasser. Applicant respectfully disagrees and traverses the Office's rejection. For at least the reasons set forth below, the rejection over the combination of Nason and Strasser does not establish a *prima facie* case of obviousness.

Nason fails to teach or suggest associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface, as positively recited by the subject matter of this claim (as amended). The Office has already admitted to this deficiency on the part of Nason (page 25 of Office action). It is important to note that the operating principles of Nason are such that decryptors are not associated each input memory surface – an SEDD of Nason is used exclusively to perform or cause any encryption and/or decryption of data. The Office is respectfully referred

to Fig. 3, and page 13, lines 15-25 of the pending Application for exemplary detail in this regard.

Also, Nason fails to teach or suggest performing an operation on the decrypted data using the GPU to provide resultant data and re-encrypting the resultant data, as positively recited by the subject matter of this claim. Nason includes no teachings directed to the re-encrypting of resultant data from a (previous) operation of a GPU. Also, Nason is devoid of any method comprising at least one of said acts of decrypting and re-encrypting taking place on a **per cache page basis**, as positively recited by the subject matter of this claim.

Strasser fails to cure the deficiencies of Nason. Specifically, Strasser fails to teach or suggest associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface, as positively recited by the subject matter of this claim. On this point, the Office asserts that Strasser teaches "using keys which are unique to each data stream for content encryption/decryption protects the content from eavesdroppers" (page 25 of Office action). Respectfully, this is not the same as, or suggestive of, the subject matter of claim 53, as amended.

More particularly, Strasser expresses no concern for *memory surfaces* or *uniquely configured decryptors* associated with each. Strasser is concerned with the frequent (i.e., every two seconds) provision of new CP keys within a dynamic data stream between two entities (Col. 4, lines 2-9 of Strasser), *not* the maintaining of data security on a memory surface (i.e., data that is not being presently communicated between entities). Furthermore, Strasser fails to teach or suggest performing an operation on the decrypted data using the GPU to provide resultant data and re-encrypting the resultant data, as positively recited by the subject matter

of this claim. Strasser is still further deficient in failing to teach or suggest at least one of said acts of decrypting and re-encrypting taking place on a per cache page basis, as positively recited by claim 53, as amended.

Accordingly, the Office's *prima facie* case of obviousness fails for at least the reasons that: 1) no combination of Nason with Strasser teaches or suggest all of the required features; and 2) the proposed modifications to the teachings of Nason are impermissible and lacking adequate support within Nason and Strasser. For at least the foregoing reasons, the Applicant asserts that claim 53, as amended, is allowable.

Claims 54-69 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 54-69 have been considered, none are seen as contributing anything of merit.

Claim 70 has been amended, and as amended recites a method comprising [added text is emphasized by underlining]:

- providing multiple input memory surfaces that are to hold encrypted data that is to be processed by a graphics processor unit (GPU) on a video card;
- ***associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface***;
- decrypting, with at least one associated decryptor, encrypted data that resides on at least one respective input memory surface;
- ***performing an operation on the decrypted data using the GPU to provide resultant data***;
- ***re-encrypting the resultant data***; and
- ***writing the encrypted resultant data to an output memory surface associated with the video card***,
- ***said acts of decrypting and re-encrypting taking place on a per cache page basis***.

[*Emphasis added.*]

In making out the rejection of this claim, the Office argues that its subject matter rendered obvious by the combination of Nason with Strasser. Applicant respectfully disagrees and traverses the Office's rejection. For at least the reasons set forth below, the rejection over the combination of Nason and Strasser does not establish a *prima facie* case of obviousness.

Specifically, no possible combination of Nason with Strasser teaches or suggests any of: 1) associating, with each input memory surface, a decryptor that is uniquely configured so as to decrypt the encrypted data that is held by the associated input memory surface; 2) performing an operation on the decrypted data using the GPU to provide resultant data; 3) re-encrypting the resultant data; and writing the encrypted resultant data to an output memory surface associated with the video card; or 4) said acts of decrypting and re-encrypting taking place on a per cache page basis, as respectively and positively recited by the subject matter of claim 70, as amended.

The Applicant asserts that the arguments provided above at least in support of claim 53, as amended, are analogous and supportive of claim 70, as amended. Additionally, the proposed modifications to the teachings of Nason are impermissible and lacking adequate support within Nason and Strasser. For at least the foregoing reasons, the Applicant asserts that claim 70, as amended, is allowable.

Claims 71-86 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 71-86 have been considered, none are seen as contributing anything of merit.

Claim 87 recites a system comprising:

- a video card;
- ***a graphics processor unit (GPU) on the video card*** and configured to process video data that is to be rendered on a display device;
- memory on the video card comprising one or more input memory surfaces configured to hold encrypted data that is to be operated upon by the GPU, and one or more output memory surfaces configured to hold encrypted resultant data that is to be rendered on the display device;
- ***a cryptographic processor on the video card and configured to control encryption and decryption on the video card, the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card***;
- each individual input memory surface having its own unique associated key for decrypting encrypted data held thereon;
- ***the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted on a per cache page basis*** so that the decrypted data can be operated upon by the GPU;
- the cryptographic processor further being configured to enable ***data that has been operated upon by the GPU to be encrypted on a per cache page basis*** to an output memory surface.

[***Emphasis added.***]

In making out the rejection of this claim, the Office argues that its subject matter rendered obvious by the combination of Nason with Garcia and Strasser. Applicant respectfully disagrees and traverses the Office's rejection. For at least the reasons set forth below, the rejection over the combination of Nason, Garcia and Strasser does not establish a *prima facie* case of obviousness.

Specifically, Nason fails to teach or suggest a graphics processor unit (GPU) on the video card and a cryptographic processor on the video card and configured to control encryption and decryption on the video card, as positively recited by the subject matter of this claim. The Office has admitted to this

deficiency of Nason (page 32 of Office action). Nason additionally fails to teach or suggest the cryptographic processor comprising a key manager for managing keys that can be utilized for encrypting and decrypting data on the video card, as positively recited by the subject matter of this claim. Nason also fails to teach or suggest the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted on a per cache page basis, as positively recited by the subject matter of claim 87. Further, Nason fails to teach or suggest data that has been operated upon by the GPU to be encrypted on a per cache page basis, as positively recited by the subject matter of this claim.

The Office argues that Garcia teaches such a cryptographic processor, because (according to the Office) Garcia teaches "that incorporating cryptographic capabilities within the GPU has many added benefits" (page 32 of Office action). However, and as argued above, any means mentioned by Garcia for executing the algorithms thereof are passing at best, and are completely lacking any specificity or detail on the order of the subject matter recited by claim 87. In any case, Garcia does not cure the deficiencies on the part of Nason with respect to the cryptographic processor and/or any of its specific capabilities as recited by claim 87.

In turn, Strasser fails to cure the mutual deficiencies of Nason and Garcia. In particular, Strasser fails to teach or suggest the cryptographic processor being configured to enable encrypted data on one or more of the input memory surfaces to be decrypted on a per cache page basis, as positively recited by the subject matter of claim 87. Further still, Strasser fails to teach or suggest data that has been operated upon by the GPU to be encrypted on a per cache page basis, as positively recited by the subject matter of this claim.

Strasser is not concerned with the particular structure and cooperative aspects of the subject matter of claim 87 because, among other things, Strasser is direct to solving a different problem (i.e., providing secure communication between remote entities) in a different way (i.e., frequent provision of new encryption keys in the data streams) than the subject matter of claim 87. Furthermore, Strasser is completely lacking any teachings or suggestions directed to means or operations performed on a per cache page basis. More to the point, Strasser is totally devoid of the terms "cache", "cache page", or any of their respective equivalents, in any context.

There is no way select elements from Nason, and then to combine those with other elements selected from Garcia, and then to combine those with still other elements selected from Strasser, in order to arrive at the subject matter as recited by claim 87, as no possible combination of Nason, Garcia and Strasser teaches or suggests all of the required features. On these grounds alone, the Applicant contends that the § 103 rejection of claim 87 is unsupportable, and must be withdrawn.

Additionally, no teachings or elements to be found anywhere in Garcia and/or Strasser override the fact that any modification to the teachings of Nason are impermissible as any such modification would result in changing the operating principle of Nason in violation of MPEP § 2143.01(VI). Thus, to modify the teachings of Nason so as to "incorporate the cryptographic processor within the GPU which is located on the graphics card", as suggested by the Office (page 33 of Office action), is not allowable and cannot be used to support a rejection of claim 87 under § 103.

Accordingly, the Office's *prima facie* case of obviousness fails for at least the reasons that: 1) no combination of Nason with Garcia and Strasser teaches or suggest all of the required features; and 2) the proposed modifications to the teachings of Nason are impermissible and lacking adequate support within Nason, Garcia and/or Strasser. For at least the foregoing reasons, the Applicant asserts that claim 87 is allowable.

Claims 88-94 are allowable at least as depending from an allowable base claim. While the particular rejections against claims 88-94 have been considered, none are seen as contributing anything of merit.

Conclusion

The claims are in condition for allowance. Accordingly, Applicant requests a Notice of Allowability be issued forthwith. If the Office's next anticipated action is to be anything other than issuance of a Notice of Allowability, Applicant respectfully requests a telephone call for the purpose of scheduling an interview.

Respectfully submitted,

Dated: 9/28/00

By: 

Lance R. Sadler
Reg. No. 38,605
(509) 324-9256